

用户指南

一、项目简介

该项目运用 java 语言实现 S-DES 算法。

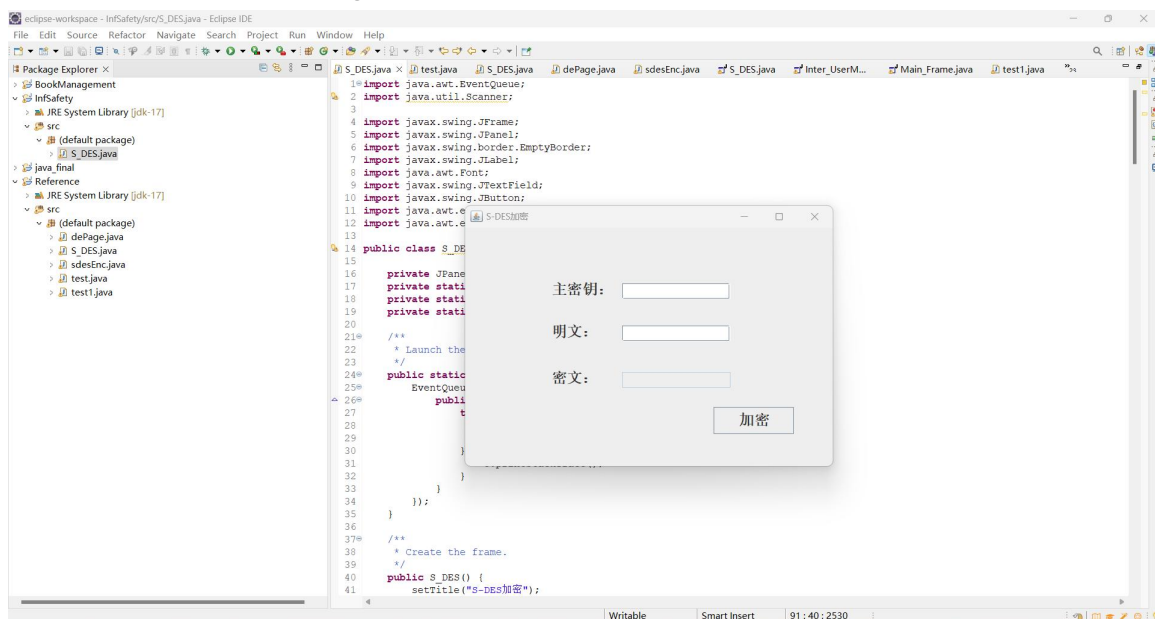
二、项目需求

1. 基础功能。编程实现 S-DES 基础加解密功能。
2. 用户界面。设计用户 GUI 界面，方便与用户进行交互。
3. 功能扩展。在明密文展现形式上进行拓展，不限于二进制的输入输出。
4. 蛮力破解。实现基于明密文对，通过穷举法暴力破解主密钥值的功能。

三、使用指南

1. 加密

用户运行程序后，出现加密 gui 界面



在“主密钥”，“明文”所对应的文本框中输入主密钥以及待加密明文，其中明文可以输入 ascii 值或 8bit 二进制值

点击“加密”按钮后，在“密文”文本框中展现加密结果



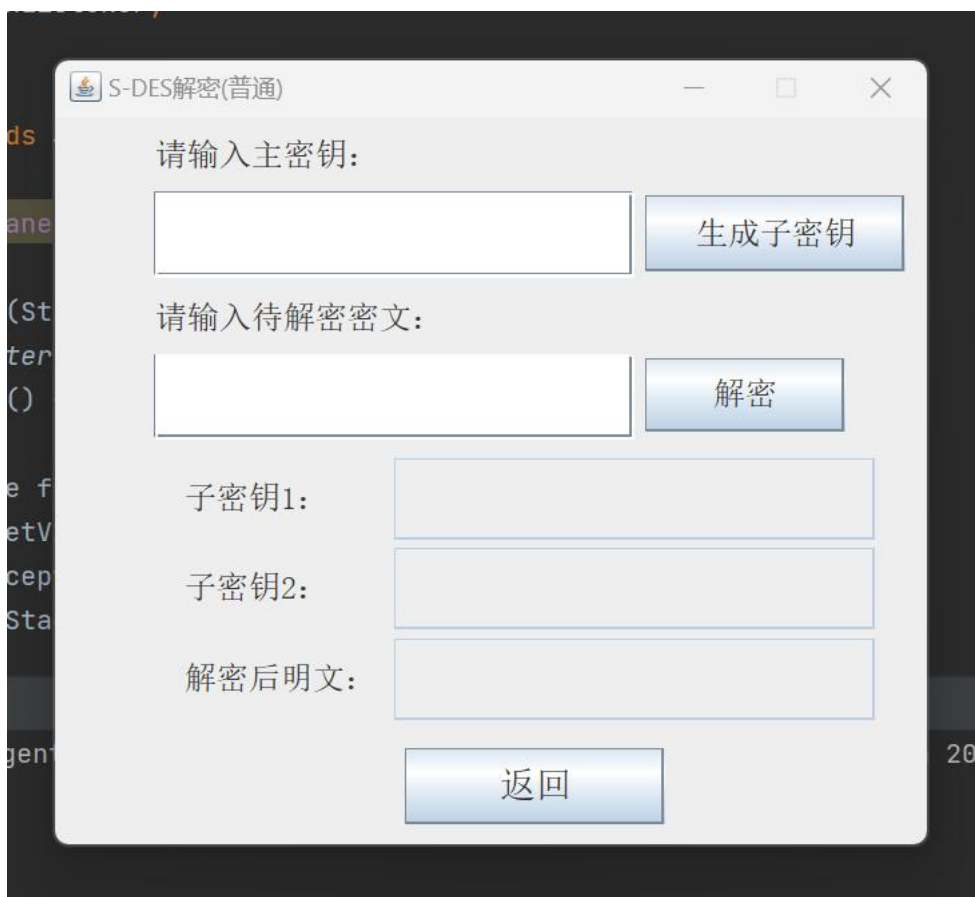
2. 解密

用户运行解密程序后，出现用户 GUI 界面

用户可以选择暴力破解、正常破解两种模式



进入正常破解界面。用户向“主密钥”，“密文”所对应的文本框中输入主密钥以及待解密密文之后，分别点击“生成子密钥”以及“解密”两个按钮，依次得到两个子密钥及明文，并于对应文本框中展现结果



S-DES解密(普通)

请输入主密钥:

1010000010

生成子密钥

请输入待解密密文:

01000100

解密

子密钥1: 10100100

子密钥2: 01000011

解密后明文: 01000011

返回

进入暴力破解界面。

暴力解密

请输入待解密密文:

请输入对应明文:

暴力解密

主密钥:

暴力解密时间:

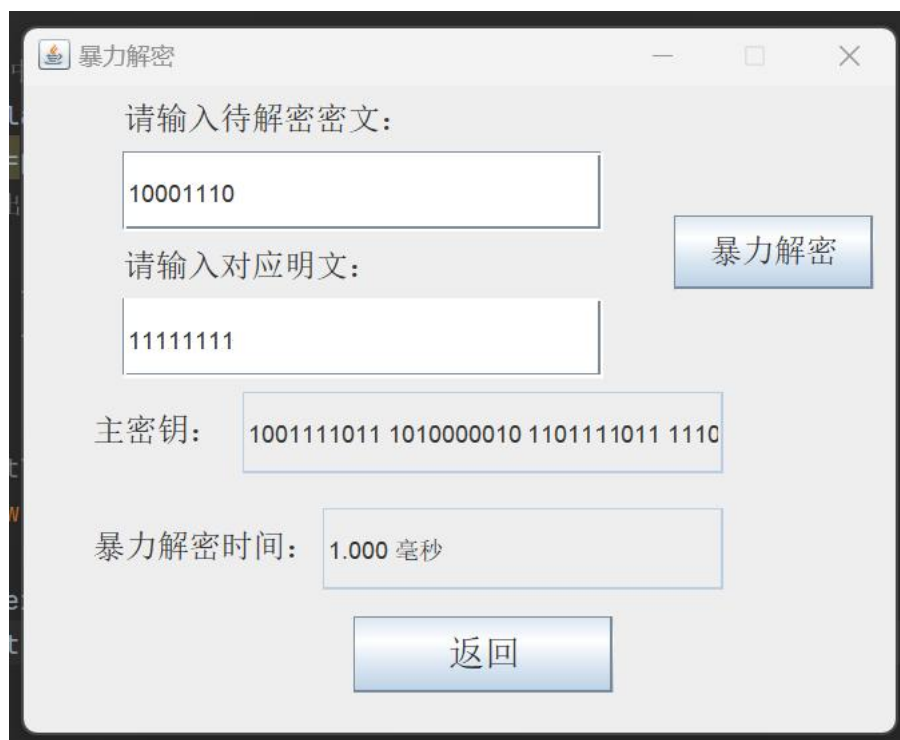
返回

用户在输入框中分别根据提示输入对应的明密文对，点击暴力解密按钮，用户将在输出框中分别看到可能的密钥和找到主密钥所需的时间。



The screenshot shows a window titled "暴力解密" (Brute Force Decryption). It contains the following elements:

- A label "请输入待解密密文:" (Please enter the ciphertext to be decrypted) above a text input field containing "11101111".
- A label "请输入对应明文:" (Please enter the corresponding plaintext) above a text input field containing "10011010".
- A blue button labeled "暴力解密" (Brute Force Decryption) to the right of the plaintext input field.
- A label "主密钥:" (Main Key) above a text output field containing "1010000010 1110000010".
- A label "暴力解密时间:" (Brute Force Decryption Time) above a text output field containing "2.000 毫秒".
- A blue button labeled "返回" (Return) at the bottom center.



The screenshot shows the same "暴力解密" window with the following updated content:

- The ciphertext input field now contains "10001110".
- The plaintext input field now contains "11111111".
- The main key output field now contains "1001111011 1010000010 1101111011 1110".
- The brute force decryption time output field now contains "1.000 毫秒".